2010

The New Employment Verification Act: The Functionality and Constitutionality of Biometrics in the Hiring Process Note

Grayson Colt Holmes

CONNECTICUT LAW REVIEW

VOLUME 43 DECEMBER 2010 NUMBER 2

Note

THE NEW EMPLOYMENT VERIFICATION ACT: THE FUNCTIONALITY AND CONSTITUTIONALITY OF BIOMETRICS IN THE HIRING PROCESS

GRAYSON COLT HOLMES

In 1990, Congress created the U.S. Commission on Immigration Reform to assess and make recommendations regarding the implementation and impact of U.S. immigration policy. Unanimously, the Commission proposed employment-based immigration reforms that have lead to the creation of E-Verify, an Internet-based electronic verification system used by employers to verify a prospective worker's eligibility. Today, the system compares a prospective worker's identification information, such as her name, date of birth, and social security number with information contained in databases housed by the Department of Homeland Security and Social Security Administration. Several members of Congress, however, have proposed legislation that would require prospective workers to submit biometric information to curb identity fraud and existing shortfalls in the verification process.

This Note examines the practical and legal implications of a nationally mandated biometric verification system and whether such a system is constitutionally viable under current Fourth Amendment jurisprudence. Ultimately this Note argues that no matter how unsettling the collection of biometric information by the government may be, at least in the employment hiring context, a nationally mandated biometric verification system will most likely pass constitutional muster.

NOTE CONTENTS

THE NEW EMPLOYMENT VERIFICATION ACT: THE FUNCTIONALITY AND CONSTITUTIONALITY OF BIOMETRICS IN THE HIRING PROCESS

GRAYSON COLT HOLMES*

I. INTRODUCTION

In April 2009, in an effort to prevent illegal immigrants from obtaining employment in the United States, six congressional legislators unveiled a plan to require prospective workers to submit biometric information through a national employment verification program.[1] The bill, which today remains in committee, threatens to foist a technology on American workers and employers that many have only seen in the movies. If the bill is passed, employers who use the verification system would collect from prospective workers not only social security numbers, birth certificates, and I-91 forms, but also biometric identification images of fingerprints, irises, and faces. A nationally mandated system that collects this information raises a host of legal questions, including whether such a requirement constitutes a search under the Fourth Amendment, and whether such a system would unduly violate societal expectations of privacy.

This Note addresses common misperceptions and legal concerns about such a nationally mandated system and examines whether such a system could work in practice and under existing Fourth Amendment jurisprudence. Part II of this Note delves into the history of employment verification in the United States and Congress's struggle to find the perfect automated system. Part III surveys the federal government's biometric activities since the September 11th terrorists attacks and evaluates current technological capabilities. Part IV explores the Fourth Amendment and privacy implications of a biometric requirement in a national employment verification program. Finally, the Note concludes that a biometric requirement has the potential to meet congressional immigration goals without impinging on the rights of prospective workers, but it cannot exist until the government strengthens existing departmental structures and allocates new resources for a national employment verification system.

The stigma attached to the government's recording of bodily

---

* University of Georgia, A.B. 2007; University of Connecticut School of Law, J.D Candidate 2011. I would like to thank Professor Kaaryn Gustafson for her insightful comments and guidance during the creation of this Note. I would also like to thank the members of the *Connecticut Law Review* for their keen eyes during the editing process, especially Ashley Schaefer for her encouragement and advice. This note is dedicated to my great-grandfather, the late Harold J. Smith. All errors are mine and mine alone.

[1] H.R. 2028, 111th Cong. (2009).

information is enormous. This Note's purpose is not to remove that stigma. Rather, it attempts to quell privacy and Fourth Amendment concerns that may arise from the use of existing biometric technology in the prospective worker-employer context. Fourth Amendment jurisprudence and societal expectations of privacy continually change with the needs of the public interest and developments in technology. This Note attempts to reconcile those competing interests and argues that a national employee verification system that extracts biometric information is constitutionally viable.

II. EMPLOYMENT VERIFICATION IN AMERICA

A. *The Evolution of Electronic Eligibility Verification Systems*

In 1990, Congress authorized a bipartisan commission, known as the U.S. Commission on Immigration Reform (Immigration Reform Commission), to evaluate the implementation and impact of U.S. immigration policy.[2] The Immigration Reform Commission first pitched the idea of a national electronic eligibility verification (EEV) system in a report to Congress in 1994.[3] The report noted that the promise of employment in the United States serves as one of the strongest attractions drawing many illegal immigrants to the country.[4] Past "open borders" immigration policies had encouraged, according to libertarian critics, undocumented immigrants to come to the United States to seek education and employment.[5] Likewise, segments of the U.S. economy have and still rely heavily on immigrants to perform tasks that many American workers were reluctant to perform.[6]

---

[2] Congress mandated the Immigration Reform Commission through the Immigration Act of 1990. The Act charged the Immigration Reform Commission to release two reports—an interim report in 1994 and a final report in 1997—detailing major immigration-related issues facing the United States. Immigration Act of 1990, Pub. L. No. 101–649, § 141(a)–(b), 104 Stat. 4978, 5001–02 (codified as amended in scattered sections of 8 U.S.C.); U.S. COMM'N ON IMMIGRATION REFORM, 1994 EXECUTIVE SUMMARY i (1994).

[3] *See* DORIS MEISSNER & MARC R. ROSENBLUM, MIGRATION POLICY INST., THE NEXT GENERATION OF E-VERIFY: GETTING EMPLOYMENT VERIFICATION RIGHT 4 (2009) (stating that the U.S. Commission on Immigration Reform recommended that Congress create an electronic eligibility verification system to end document fraud); U.S. COMM'N ON IMMIGRATION REFORM, *supra* note 2, at xiii–xviii (explaining the benefits of a computerized verification system and the proposed features of a pilot program).

[4] U.S. COMM'N ON IMMIGRATION REFORM, *supra* note 2, at xii (stating the need to decrease the employment magnet).

[5] *See* Jim Harper, *Electronic Employment Eligibility Verification: Franz Kafka's Solution to Illegal Immigration*, 612 CATO INST. POL'Y ANALYSIS 1, 4 (2008), *available at* http://www.cato.org/pub_display.php?pub_id=9256 (explaining the "open borders" policy during the early part of American history and how Congress passed legislation encouraging immigration to overcome the labor shortage caused by the Civil War).

[6] *See, e.g.*, PARR ROSSON ET AL., NAT'L MILK PRODUCERS FED'N, THE ECONOMIC IMPACTS OF IMMIGRATION ON U.S. DAIRY FARMS 2 (2009), *available at* http://nmpf.org/latest-news/press-releases/jun-2009/nmpf-study-finds-dairy-farms-rely-heavily-on-foreign-workers (stating that dairy

The Immigration Reform Commission noted that one goal that should underpin any successful national immigration policy is "reducing the employment magnet."[7] To this end, the Immigration Reform Commission recommended a national program that hinged its success on worksite and employer enforcement. The recommended plan called for employers to leverage a computerized national identity verification program to curb identity fraud, while the federal government would ensure employer compliance through the imposition of penalties and fines for employers who employed unauthorized workers.[8]

In response to the Immigration Reform Commission's report, Congress created three electronic verification pilot programs to test the effectiveness of a national EEV system in which employers could voluntarily enroll.[9] It charged the Immigration and Naturalization Services (INS) and Social Security Administration (SSA) with the task of commencing the three programs, and all three were fully implemented by 1997.[10] Of the three programs, the "Basic Pilot" (renamed "E-Verify") proved the most

---

farmers employ 57,000 foreign-born immigrants or forty-one percent of their workforce and that eliminating immigrant labor would reduce the U.S. dairy herd by 1.34 million head, reduce milk production by 29.5 billion pounds, and reduce the number of dairy farms by 4,532, increasing milk prices by about sixty-one percent). *But see* STEVEN A. CAMAROTA & KAREN JENSENIUS, CTR. FOR IMMIGRATION STUDIES, JOBS AMERICANS WON'T DO?: A DETAILED LOOK AT IMMIGRANT EMPLOYMENT BY OCCUPATION 1–2 (2009), *available at* http://www.cis.org/illegalimmigration-employment (stating that a 2005–2007 survey found that there were only a small number of majority-immigrant occupations and that immigrants do not take jobs Americans want).

[7] U.S. COMM'N ON IMMIGRATION REFORM, *supra* note 2, at xii; *see also Save America Comprehensive Immigration Act of 2007: Hearing on H.R. 750 Before the Subcomm. on Immigration, Citizenship, Refugees, Border Sec., and Int'l Law of the H. Comm. on the Judiciary,* 110th Cong. 187 (2007) (statement of T.J. Bonner, National President, National Border Patrol Council of the American Federation of Government Employees AFL-CIO) (stating that proposed solutions have failed to curb illegal immigration because they have not "reduced the employment magnet"). Notably, only one federal court has acknowledged the "employment magnet" that Congress has "endeavored to turn-off." *See* Am. Friends Serv. Comm. v. Thornburgh, 718 F. Supp. 820, 822–23 (C.D. Cal. 1989) (deferring to the government's overriding interest in immigration control and upholding sanctions against an employer who knowingly employed an illegal alien because reversing sanctions would "reactivat[e] the employment 'magnet'").

[8] U.S. COMM'N ON IMMIGRATION REFORM, *supra* note 2, at xiii–xiv, xix–xx.

[9] MEISSNER & ROSENBLUM, *supra* note 3, at 4; Harper, *supra* note 5, at 5. These three programs are the Citizen Attestation Verification Pilot Program (CAVPP), the Machine-Readable Document Pilot Program (MRDPP), and the Basic Pilot Program (E-Verify). *Id.* at 5. The blueprints for each plan were laid out in Title IV of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996. Pub. L. 104-208, §§ 401–05, 110 Stat. 3009-546, 655–66 (1996) (codified at 8 USC § 1324a et seq.).

[10] Lindsay L. Chichester & Gregory P. Adams, *The State of E-Verify: What Every Employer Should Know*, 56 FED. LAW., July 2009, at 50, 50. CAVPP allowed workers to attest to their citizenship status, which was then electronically checked against information in INS databases. Unsurprisingly, ineligible workers attested to being citizens, and many employers rarely sought out fraud. Some employers, however, discriminated against work-authorized noncitizens because of the liability risks associated with the worker's presence. MRDPP was initiated in Iowa because of the state's machine-readable driver's licenses and ID cards. The program suffered from technical difficulties in reading the IDs and was undermined by the state's transition away from using SSNs on driver's licenses. Both CAVPP and MRDPP were terminated by the Department of Homeland Security in 2003. Harper, *supra* note 5, at 5.

successful and is the current model of success for Congress's national immigration reform campaign.[11]

E-Verify was first implemented in the five states that Commission officials said "had the highest estimated numbers of undocumented immigrants: California, Florida, Illinois, New York, and Texas."[12] Employers in those states were not required to use the system, but instead voluntarily registered to participate.[13] Two years later, the program expanded to include Nebraska.[14] By 2003, E-Verify had expanded to all fifty states and the two other pilot programs had been discontinued.[15] Although the INS initially oversaw E-Verify's implementation, it was reconfigured in the wake of the 9/11 attacks, and the Department of Homeland Security (DHS) and the SSA currently operate E-Verify's internet-based database.[16]

E-Verify works by checking information—name, date of birth, social security number (SSN) and, for non-citizens, alien identification number—provided to the employer by the prospective worker.[17] Employers must "submit this information through a secure website within three days after [the] worker is hired."[18] The program then checks the worker-provided information against the SSA's main database, called "Numident," if she is a citizen, or, if she is a noncitizen, against the DHS composite system, called the "Verification Information System" or "VIS."[19] If the worker's information matches the records on either Numident or VIS, E-Verify returns a confirmation to the employer through the website, and the worker is cleared to work.[20] When the information cannot be verified through the database, E-Verify responds with a tentative non-confirmation (TNC).[21] The law then shifts the burden to the worker; the employer must inform the worker of her status and provide her with procedural instructions to contest

---

[11] Chichester & Adams, *supra* note 10, at 50; *see also* MEISSNER & ROSENBLUM, *supra* note 3, at 4 (stating that Basic Pilot became a national voluntary program in 2003 and now operates as E-Verify); Harper, *supra* note 5, at 5 (stating that Basic Pilot, which was renamed "E-Verify," "is the remaining effort to verify work eligibility electronically").

[12] Chichester & Adams, *supra* note 10, at 50. In May of 2008, E-Verify had been used by most states on a voluntary basis, while ten required the use of E-Verify for public or private employers. Lizzette Romero, Note, *E-Verify: Expansion and Recent Developments*, 4 ISJLP 605, 610 (2008).

[13] Chichester & Adams, *supra* note 10, at 50.

[14] *Id.*

[15] *Id.*; Harper, *supra* note 5, at 5.

[16] Peter F. Asaad & Stephanie S. Wesley, *E-Verify: A Trojan Horse at the Employer's Doorstep*, BUS. L. BRIEF, Fall 2008, at 26, 26; Chichester & Adams, *supra* note 10, at 50. The INS was one of the twenty-two departments consolidated into DHS after the 9/11 attacks. *See infra* Part III.B.2 for a description of the DHS's biometrics program.

[17] MEISSNER & ROSENBLUM, *supra* note 3, at 4.

[18] *Id*.

[19] *Id*.

[20] *Id.*; Harper, *supra* note 5, at 5.

[21] MEISSNER & ROSENBLUM, *supra* note 3, at 4; Harper, *supra* note 5, at 5.

the TNC in case of an error.[22] The worker has eight days to contest the TNC.[23] If the worker fails to or cannot challenge the TNC, then E-Verify issues a final non-confirmation and the employer is required to either terminate the worker or notify the DHS that it is employing a noncompliant worker, subjecting the employer to criminal and civil penalties.[24] Additionally, the E-Verify program obliges participating employers to permit the SSA and DHS to make periodic "work site[]" visits and to "make employment and E-Verify related records available" at the Department's request.[25]

B. *The Move To Nationalize EEV*

On June 9, 2008, DHS Secretary Michael Chertoff remarked at the State of Immigration Address that the "[o]ne critical tool for our success [in curbing illegal immigration] is giving the employer the means to check whether the applicant for a job is in fact presenting a valid social security number and name that match what is in our government databases."[26] In another speech on August 10, 2007, he outlined a plan to expand EEV and its underlying policy in three key areas.[27] First, DHS would designate E-Verify as the EEV system in which all federal contractors and vendors must participate.[28] This expansion added a potential 200,000 companies to the 52,000 who were using E-Verify at that time, bringing the total number of American companies using the system to 3.5 percent.[29] Second, Secretary Chertoff announced DHS's creation of a "no-match" regulation increasing an employer's liability if its workers' names and SSNs do not correspond to SSA records. The new policy would raise penalties by twenty-five percent and expand criminal investigations into employers who were charged with violating the DHS policy.[30] Third, Secretary Chertoff advocated integrating information in the national database utilized by E-

---

[22] MEISSNER & ROSENBLUM, *supra* note 3, at 4–5; Harper, *supra* note 5, at 5.

[23] MEISSNER & ROSENBLUM, *supra* note 3, at 5; Harper, *supra* note 5, at 5.

[24] MEISSNER & ROSENBLUM, *supra* note 3, at 5; Harper, *supra* note 5, at 5. Workers who receive TNCs and fail to challenge them comprise almost eighty-five percent of TNC cases. MEISSNER & ROSENBLUM, *supra* note 3, at 5. An employer is subjected to fines that range "from $500 to $1,000 for each failure to notify the DHS. If the employer continues to employ the worker after [receiving] a final nonconfirmation, there is a rebuttable presumption that the employer is knowingly employing an unauthorized worker." Chichester & Adams, *supra* note 10, at 51.

[25] Chichester & Adams, *supra* note 10, at 51 (internal quotation marks omitted).

[26] Michael Chertoff, Homeland Sec. Sec'y, & Carlos Gutierrez, Commerce Sec'y, State of Immigration Address (June 9, 2008) [hereinafter Chertoff & Gutierrez, Immigration Address], *available at* http://www.dhs.gov/xnews/releases/pr_1213101513448.shtm.

[27] Michael Chertoff, Homeland Sec. Sec'y, & Carlos Gutierrez, Commerce Sec'y, Press Conference on Border Security and Administrative Immigration Reforms (Aug. 10, 2007) [hereinafter Chertoff & Gutierrez, Border Security], *available at* http://www.dhs.gov/xnews/releases/pr_1186781502047.shtm.

[28] Harper, *supra* note 5, at 6; Chertoff & Gutierrez, Border Security, *supra* note 27.

[29] Harper, *supra* note 5, at 6.

[30] *Id.*; Chertoff & Gutierrez, Border Security, *supra* note 27.

Verify with other information databases.[31] This would include access to information from visas, passports, and state motor vehicle records, which would "lay the ground work for further expansion."[32]

Although Congress has yet to pass a law requiring all employers to use E-Verify, recently several bills have been introduced in both the House and Senate to nationalize some form of E-Verify. One legislator commented on how there were currently eleven different proposals before the House Judiciary Subcommittee suggesting reforms to E-Verify in preparation for a national EEV program.[33] In April 2009, Representative Gabrielle Giffords of Arizona and Representative Sam Johnson of Texas introduced House Resolution 2028, the New Employee Verification Act (NEVA), which would extend the E-Verify program five more years and create a new, more secure verification program in which employers could also enroll.[34] The new system, like E-Verify, would rely on the SSA and DHS databases and include biometric information.[35]

In a hearing held in July 2009, Senator Charles Schumer endorsed passing a bill that would create a "tough, fair, and effective employment verification system," and Representative Luis Gutierrez stated that an "employment verification system must be part of [any] comprehensive immigration reform" package.[36] Senator Schumer outlined ten characteristics, including requiring biometric information from prospective workers, that he said were needed for a successful EEV system.[37] Several legislators also voiced their support for a national EEV program and

---

[31] Chertoff & Gutierrez, Border Security, *supra* note 27.

[32] Harper, *supra* note 5, at 6 (quoting the White House's statement in a fact sheet released August 10, 2007). Note that the fact sheet Harper cites is now available through the DHS website at http://www.dhs.gov/xnews/releases/pr_1186757867585.shtm.

[33] *Electronic Employment Verification Systems: Needed Safeguards to Protect Privacy and Prevent Misuse: Hearing Before the Subcomm. on Immigration, Citizenship, Refugees, Border Sec., and Int'l Law of the H. Judiciary Comm.*, 110th Cong. 6 (2008) [hereinafter *Electronic Employment Verification Systems*] (statement of Rep. Conyers).

[34] H.R. 2028, 111th Cong. §§ 101, 102 (2009); Chichester & Adams, *supra* note 10, at 61.

[35] H.R. 2028 § 103(b)(2)(A); Chichester & Adams, *supra* note 10, at 61.

[36] *Ensuring a Legal Workforce: What Changes Should Be Made to Our Current Employment Verification System?: Hearing Before the Subcomm. on Immigration, Refugees and Border Sec. of the S. Judiciary Comm.*, 111th Cong. 1–2, 10 (2009) [hereinafter *Ensuring a Legal Workforce*] (statements of Sen. Schumer, Chairman, S. Judiciary Subcomm., and Rep. Gutierrez).

[37] *Id.* at 2–4. The characteristics outlined by Senator Schumer are: (1) requiring employers to check information against a federal immigration system; (2) using biometric identifiers to identify prospective workers; (3) requiring employers to use the system on all prospective workers regardless of immigration or citizenship status; (4) creating an inexpensive, easy-to-use, and quick program; (5) exonerating employers who hire illegal workers because EEV returns false positives; (6) punishing employers not using EEV when they hire illegal workers and employers using EEV when they "knowingly hire illegal workers"; (7) funding the system with fees paid by non-citizens when they obtain work permits and authorization; (8) ensuring significant and substantial protections built into EEV to prevent workers from being erroneously denied work and allowing workers to work while resolving TNCs; (9) requiring security checks when biometric information is collected and entered into the system; and (10) safeguarding the privacy and civil liberties of workers and only allowing the system to be used for employment verification purposes.

reforms that could make such a system possible, including the addition of a biometric element.[38]

The House Judiciary Committee held a similar hearing where representatives also expressed support for nationalizing EEV. The discussion centered around existing shortfalls in E-Verify and reforms necessary to expand the program nationally.[39] Representative Heath Shuler of North Carolina advocated for phasing in a mandatory EEV system within a four-year period.[40] Representative Steven King of Iowa suggested incorporating naturalization databases into the existing SSA and DHS databases used by E-Verify.[41]

Legislation has also been proposed that would have required new-hires to have a "REAL ID Act-compliant" card.[42] The REAL ID Act, passed in 2005, imposes security, authentication, and issuance procedural standards for state driver's licenses and state ID cards.[43] Most states, however, have yet to comply with the Act. In April 2008, all fifty states had received or applied for extensions beyond the May 11, 2008 deadline.[44] By October of 2009, twenty-six states had adopted resolutions that declared their intent not to comply with the program.[45]

Several states have passed legislation mandating that certain employers participate in the E-Verify program. As of November 2010, Arizona, Mississippi, South Carolina, and Utah required all employers in those

---

[38] *Id.* at 5, 7, 9. These include Senators John Cornyn, Jeff Sessions, and Representative Luis Gutierrez, who was a witness at the Senate hearing.

[39] *Electronic Employment Verification Systems*, *supra* note 33, at 1.

[40] *Id.* at 33.

[41] *Id.* at 54.

[42] S. 1348, 110th Cong. (2007). Called the "Comprehensive Immigration Reform Act of 2007," the bill was eventually defeated when it failed to garner the sixty votes necessary to move it from debate to passage. Michael Sandler & Jonathan Allen, *Senate Gives Up on Immigration Bill*, CONG. Q. TODAY, June 7, 2007.

[43] Real ID Act of 2005, Pub. L. 109-13, § 202, 119 Stat. 231, 312–15 (codified as amended in scattered sections of 8 U.S.C.); Mimi Hall, *States Get 'Real ID' Extensions*, USA TODAY, Apr. 2, 2008, *available at* http://www.usatoday.com/news/nation/2008-04-02-realid_N.htm.

[44] Real ID Act § 202(a)(1) (providing that the requirements will go into effect three years from the May 11, 2005 date of enactment); Hall, *supra* note 43 (stating that DHS granted all 50 states extensions).

[45] *See Anti-Real ID Legislation in the States*, REALNIGHTMARE.ORG, http://www.realnightmare.org/news/105/ (last visited Nov. 19, 2010) (displaying states who passed legislation prohibiting REAL ID or resolutions denouncing REAL ID); *see also* Jaikumar Vijayan, *Obama Will Inherit a Real Mess on REAL ID: The Effort To Impose National Standards for Photo IDs Remains a Bone of Contention Between Federal and State Officials*, COMPUTERWORLD, Dec. 22, 2008, *available at* http://www.computerworld.com/s/article/331497/Obama_Will_Inherit_A_Real_Mess_On_Real_ID (discussing Arizona Governor Janet Napolitano's signing of an Arizona bill barring the state from participating in the program). Napolitano, a strong opponent of the REAL ID program, was appointed as head of DHS when President Obama took office, placing the future of the Act in uncertain waters. *Id*. *But see* Dennis Myers, *REAL ID Is Coming: As Obama and Congress Slow a Federal Driver License to a Crawl, Gibbons and DMV Race Ahead*, NEWSREVIEW.COM (Feb. 11, 2010), http://www.newsreview.com/reno/content?oid=1369527 (reporting on the Nevada Governor's push for REAL ID).

states to enroll in E-Verify.[46] Georgia, Idaho, Missouri, and Nebraska currently require that all state offices and all or most state contractors participate in the program, while Minnesota and Rhode Island have extended the mandate to only their executive branches and state contractors.[47] North Carolina, Oklahoma, and Virginia have also passed legislation that requires state offices to use E-Verify.[48] Tennessee provides incentives for private employers who voluntarily use the program and immunizes employers enrolled in the E-Verify program from state

---

[46] *See* Legal Arizona Workers Act, ARIZ. REV. STAT. ANN. § 23-214(A) (Supp. 2009) ("[E]very employer . . . shall verify the employment eligibility of the employee through the e-verify program."); Mississippi Employment Protection Act, MISS. CODE ANN. § 71-11-3(4)(b)(i) (2010) ("Every employer shall register with and utilize the status verification system to verify the federal employment authorization status of all newly hired employees."); South Carolina Illegal Immigration Reform Act, S.C. CODE ANN. § 8-14-20(A) (Supp. 2009) ("[E]very public employer shall register and participate in the federal work authorization program to verify the employment authorization of all new employees."); UTAH CODE ANN. § 13-47-201(1) (LexisNexis Supp. 2010) ("A private employer who employs 15 or more employees . . . may not hire a new employee . . . unless the private employer . . . uses the status verification system to verify the federal legal working status of the new employee . . . .").

[47] *See* Georgia Security and Immigration Compliance Act, GA. CODE ANN. § 13-10-91(a)–(b) (West Supp. 2009) ("Every public employer . . . shall register and participate in the federal work authorization program to verify employment eligibility of all newly hired employees. . . . No public employer shall [contract] for the physical performance of services . . . unless the contractor . . . participates in the federal work authorization program . . . ."); Idaho Exec. Order No. 2006–40 (May 29, 2009), *available at* http://gov.idaho.gov/mediacenter/execorders/eo09/eo_2009_10.html ("The Division of Human Resources shall . . . verify and ensure that all new employees with any agency of the State of Idaho are eligible for employment under federal and state law. . . . [A]ll contractors and subcontractors [must] declare to the contracting state agency that they have substantiated that all employees providing services"); MO. ANN. STAT. § 285.530.2 (West Supp. 2010) ("As a condition for the award of any contract or grant in excess of five thousand dollars . . . the business entity shall . . . affirm its enrollment and participation in a federal work authorization program with respect to the employees working in connection with the contracted services."); NEB. REV. STAT. § 4-114(2) (Supp. 2009) ("Every public employer and public contractor shall register with and use a federal immigration verification system to determine the work eligibility status of new employees physically performing services within the State of Nebraska."); Minn. Exec. Order No. 08-01 (Jan. 7, 2008), *available at* http://www.governor.state.mn.us/mediacenter/pressreleases/printerfriendly/PROD008598.html ("Requiring all hiring authorities within the executive branch of state government to use the federal electronic work verification program ('E-Verify')."; R.I. Exec. Order No. 08-01, *available at* http://www.governor.ri.gov/documents/executiveorders/2008/01_illegal_immigration_control_order.pdf ("The Deparment of Administration shall register and use the federal government's E-Verify program . . . [and] shall require that all persons and business . . . doing business with the state of Rhode Island also register with . . . the E-Verify Program.").

[48] N.C. GEN. STAT § 126-7.1(f) (2010) ("Each State agency, department, institution, university, community college, and local education agency shall verify, in accordance with the Basic Pilot Program administered by the United States Department of Homeland Security . . . ."); The Oklahoma Taxpayer and Citizen Protection Act of 2007, OKLA. STAT. tit. 25, § 1313.A (West 2007) ("Every public employer shall register with and utilize a Status Verification System . . . ."); VA. CODE ANN § 40.1–11.2 (Supp. 2010) ("All agencies of the Commonwealth shall be enrolled in the E-Verify program by December 1, 2012 . . . ."). A U.S. District Court has delayed enforcement of the law in Oklahoma by granting a preliminary injunction against it and, therefore, it is not in effect. Chamber of Commerce of the U.S. v. Henry, No. CIV-08-109-C, 2008 WL 2329164, at *8 (W.D. Okla. June 4, 2008). In February 2010, the Tenth Circuit, reversing in part and affirming in part the District Court's decision, upheld the injunction. Chamber of Commerce of the U.S. v. Edmondson, 742 F.3d 742, 771 (10th Cir. 2010).

sanctions.[49] Likewise, Arkansas, Indiana, Ohio, Rhode Island, and Wyoming have introduced legislation that would mandate EEV participation for some or all of the employers in their state.[50] A number of local governments have also initiated some mandatory EEV requirements in the absence of federal law. For example, the city of Mission Viejo, California requires employers that have contracts with the city to confirm worker eligibility through E-Verify.[51] Columbia County, Oregon also passed an ordinance requiring all county employers to use E-Verify.[52]

Only one state has reacted adversely to the voluntary program. The Illinois legislature passed a statute that banned employers from using E-Verify until SSA and DHS could provide a response within three days in ninety-nine percent of the cases that receive a TNC. In March 2009, however, a U.S. District Court struck down the Illinois provision, allowing employers to enroll voluntarily in the program or to opt-out.[53]

C. *Assessing the Current State of E-Verify*

E-Verify offers some advantages against legal liability to employers and workers who voluntarily participate in the program. First, when an employer hires a worker authorized by the system, the employer is presumed to have not knowingly hired an undocumented worker should an action be brought against that employer.[54] This is particularly important as DHS worksite raids are unlikely to cease during the Obama administration.[55] There is also a special benefit for U.S. college graduates who are foreign nationals and who would like to extend their stays in the United States: employers who participate in E-Verify may extend the former student's "Optional Practical Training" work permit for an additional seventeen months.[56] Several states have also extended benefits to employers who participate in the program, offering state contracts exclusively to those employers or immunizing them from legal liability.[57]

During the program's thirteen-year stint, many enhancements and corrections have been made, offering a systematic stability that could work

---

[49] TENN. CODE ANN. § 50-1-103(d) (2008) ("A person has not violated subsection (b) . . . if the person verified the immigrant status of the person . . . by using the federal electronic work authorization verification service provided by the United States department of homeland security . . . .").

[50] Chichester & Adams, *supra* note 10, at 53

[51] *Id.*

[52] *Id.*

[53] United States v. Illinois, No. 07-3261, 2009 WL 662703, at *3 (C.D. Ill. Mar. 12, 2009).

[54] Chichester & Adams, *supra* note 10, at 51.

[55] Dawn Lurie, *Employers Beware: DHS's Shifting Priorities in Immigration Worksite Enforcement*, SECURITY DEBRIEF (June 10, 2009), http://securitydebrief.adfero.com/2009/06/10/employers-beware-dhss-shifting-priorities-in-immigration-worksite-enforcement/.

[56] Chichester & Adams, *supra* note 10, at 51.

[57] See *supra* notes 47–49 and accompanying text for a discussion on various state requirements and incentives for using E-Verify.

on a national level.[58] Jonathan Scharfen, Acting Director of the United States Citizenship and Immigration Services ("USCIS"), testified to the House Judiciary Subcommittee that the government has made significant improvements to E-Verify, which have decreased mismatches and other mistakes in the databases, enhanced user ability, reduced typographical errors, protected data privacy, and deterred document fraud.[59] USCIS plans to integrate passport and visa data into the program, to strengthen the system's accuracy.[60] Also, because many employers and government users are familiar with E-Verify, a national implementation may cost less than creating a new one from the ground up.

E-Verify does, however, exhibit problems and place burdens on various entities, which would be exacerbated if the number of users increased exponentially, should Congress require all employers to participate. First, the program places significant burdens on the employer. Each participant must obtain photocopies of a new employee's Employment Authorization Card or Permanent Residence Card issued by DHS, which is ordinarily not required by federal law.[61] For small business owners—who lack photocopying resources—such a requirement creates time and monetary costs. Large companies may also be burdened by the initial implementation cost, as hiring processes would need to be restructured, new documents would need to be created, and employee training would be necessary.[62] Participation in the program exposes employers to SSA or DHS worksite visits that can disrupt business operations and further expose a business to other civil or criminal

---

[58] Many legislators have also lauded the benefits of E-Verify in comparison to other national verification programs. For example, Representative King said the system provides "a fast and easy method" to verify a prospective worker's employability, which he claimed was evidenced by the 1,000 employers who have signed up weekly to participate in the voluntary program. *Electronic Employment Verification Systems*, *supra* note 33, at 3–4. Representative Lamar Smith of Texas reported that employers using E-Verify did not feel overburdened and were generally satisfied with the system's performance. *Id.* at 5. He added that the program rejected less than one percent of persons eligible to work and accepted over ninety-seven percent of workers born outside the United States. *Id.*

[59] *Id.* at 46–47; MARC R. ROSENBLUM, MIGRATION POLICY INST., THE BASICS OF E-VERIFY, THE US EMPLOYER VERIFICATION SYSTEM (2009), http://www.migrationinformation.org/Feature/display.cfm?ID=726. In the last six years, several improvements have been made to E-Verify: (1) in 2005, E-Verify switched from a phone-based system to an internet-based one making data and usability easier; (2) in 2008, DHS improved the communication links among its databases allowing real-time updates of new immigrants' information; (3) in 2007, a photo-screening tool was added to limit identity fraud; and (4) in 2008, DHS allowed for DHS database confirmations, even when SSA databases had not been updated to reflect a new citizen's changed status. *Id.*

[60] *Electronic Employment Verification Systems*, *supra* note 33, at 46 (statement of John Scharfen, Acting Director, USCIS).

[61] Chichester & Adams, *supra* note 10, at 51.

[62] Asaad & Wesley, *supra* note 16, at 27. The American Council on International Personnel stated that significant implementation costs could be expected for large and complex organizations. These include performing legal reviews, altering the process for hiring workers, developing protocols for resolving TNC and final nonconfirmations, and training staff. *Id*. One company reported that it cost $40,000 annually to outsource E-Verify services. *Id*.

penalties.[63] Enrollment itself does not immunize an employer from penalties, and many employers may falsely believe that once they enact the system there is no need to continue to heed existing immigration laws. As a national E-Verify system has not been tested, screening problems may create chaos for the participating employer, SSA, and DHS offices.

Second, the mandate also places burdens on the federal government and taxpayers. A Government Accountability Office (GAO) study found that mandating E-Verify participation would "substantially increase" the demands on DHS and SSA resources.[64] A mandated program could cost DHS over $400 million annually and add 3.6 million additional visits or phone calls to SSA field offices.[65] As things stand, many of the TNC-initiated investigations are false positives, yielding few final non-conformations.[66] Most TNC-generated inquiries stem from changes in citizenship status or in names that have not been updated in the SSA database.[67] Assuming nationwide enrollment, the current one percent error rate would affect 600,000 workers per year.[68] That error rate would also likely increase as a mandatory system would increase enrollment, placing greater strain on the system's infrastructure. Staffing universal enrollment could also create new and unforeseeable types of errors.[69]

Aside from negative effects on employers and government resources, E-Verify also places burdens on the prospective workers, who are screened when applying for jobs. Many foreign-born applicants are particularly vulnerable to misspellings and incorrect name order in the SSA and DHS databases.[70] This type of error usually leads to a TNC, which initially prevents the worker from securing employment.[71] Further, E-Verify requires the employer to inform the worker of the TNC.[72] Should an employer fail to notify the worker, the worker may miss her opportunity to

---

[63] A DHS raid on six Swift & Co. (now JBS Swift & Co.) meat processing plants, for example, cost the company 1,200 workers and fifty-three million dollars, despite the fact that the company had used E-Verify for many years. *Id.* at 26.

[64] Romero, *supra* note 12, at 612. Despite the fact that some companies do everything permissible to ascertain the immigration status of all workers through E-Verify and still enjoy some legal benefits from participation, they are not immune to the economic impacts of raids when they unknowingly hire illegal workers.

[65] *Id*.

[66] *Id.* at 613. Other errors can occur as a result of employer mistakes and "[r]oot errors" in the database, which are underlying mistakes in the SSA and DHS databases. MEISSNER & ROSENBLUM, *supra* note 3, at 8 n.26.

[67] Romero, *supra* note 12, at 613.

[68] MEISSNER & ROSENBLUM, *supra* note 3, at 8.

[69] *Id*. at 8 n.27 (stating that the GAO estimates that verification of all new hires would require E-Verify to process sixty-three million queries per year).

[70] Because many names have multiple spellings, some cultures use different name orders, and some languages require transliteration from non-Latin alphabets, foreign-born citizens are more likely to face such errors. *Id.* at 6.

[71] *See id.* at 5–6 (stating that "errors may prevent US citizens and other legal workers from initially–or occasionally ever–being confirmed").

[72] *Id.* at 5.

contest the TNC and then lose her job. The program also burdens the worker with the responsibility of contesting the TNC.[73] This responsibility disadvantages the worker, who may have to miss important training or take unpaid time off to contact the USCIS or SSA to correct the error.[74] The TNC may also go unresolved if the prospective worker is unfamiliar with the resolution process. These problems disproportionately affect legal immigrants, foreign-born citizens, and other minorities.[75]

As many in Congress have noted, the current E-Verify system also suffers from inherent vulnerabilities that undocumented workers can easily exploit. For example, although the system can determine whether a SSN provided by a prospective worker is valid, it cannot determine whether that SSN actually belongs to that worker.[76] E-Verify, therefore, lacks the ability to ensure that the worker presenting the SSN is the actual person to whom the information belongs.[77]

Other E-Verify shortcomings stem from its reliance on employer enforcement. The participating employer is required to collect and examine all worker documents at the time of hire.[78] The employer must attest under penalty of perjury that it has made a good faith examination of the worker's documents, that it found them to be genuine, and that the worker appears to be eligible to work.[79] Employers, however, often fail to accurately do this, because at the opening of the employment relationship, the employer has little incentive to examine a prospective worker's identity.[80] The "identification-by-card process" also contains many weaknesses that either party might exploit.[81] Along the same lines, the system is vulnerable to identity fraud initiated by the employer, because the employer stands as a first-line enforcer of E-Verify's policies with

---

[73] *See id.* (explaining that "[w]orkers have eight business days to contact the appropriate federal agency and initiate a challenge to the TNC, which generally requires calling [USCIS] or visiting an SSA field office").

[74] *Id*. at 6.

[75] *See id.* at 6 n.19 (stating that "[t]he known error rate (i.e., corrected TNCs) in 2006–2007 was *30 times* higher for foreign-born than native-born workers, and *98 times* higher for naturalized US citizens than for native-born citizens").

[76] Asaad & Wesley, *supra* note 16, at 27. Many workers who were caught in a DHS raid at Howard Industries had illegally obtained and used valid Social Security numbers. *Id*.

[77] As Michael Aytes, Acting Director of the USCIS, noted, the system was not designed to detect identity theft, but that recently a photo screening tool was added to "combat document and identity fraud." *Ensuring a Legal Workforce*, *supra* note 36, at 13.

[78] MEISSNER & ROSENBLUM, *supra* note 3, at 9.

[79] Harper, *supra* note 5, at 11.

[80] *See id*. (explaining that the initial interaction between an employer and prospective worker is not like ongoing personal relationships, and that the prospective worker of a low-skill job "proffers his or her identity for the first time").

[81] *See, e.g.*, *id.* at 11–13 fig.1 (describing "the three steps by which a card transfers identity information from the ID subject (the cardholder) to the ID verifier (or relying party)" and their vulnerabilities).

little, if any, government oversight.[82] E-Verify cannot prevent the employer from hiring a worker "under the table" when she has knowledge of an undocumented applicant but needs the worker's services.[83]

D. *House Resolution 2028*

In June 2008, the House Judiciary Subcommittee held a public hearing consisting of three panels to address the need for an EEV system that would protect worker privacy and prevent employer misuse.[84] At the time of the hearing, there were eleven bills pending before the Judiciary Committee, each proposing a nationally mandated EEV system.[85] One bill, introduced by Representative Gabrielle Giffords of Arizona, included the option for a worker to "lock" her identity after submitting her SSN to an employer for verification.[86] Another proposal incorporated a photograph-screening tool that would compare the photos of passports on record with photos presented by the worker.[87] But the most promising solution presented to combat identify fraud was House Bill 2028 ("NEVA"), a bipartisan bill that would incorporate biometric identification information such as fingerprint images or retinal scans of the prospective worker into E-Verify.[88]

NEVA extends E-Verify for another five years.[89] The bill requires employers who must participate, or who are voluntarily participating, in a verification program, to use either E-Verify or the Secure Employment Eligibility Verification System ("SEEVS"), an automated employment verification system established by NEVA.[90] Like E-Verify, SEEVS requires employers to check information provided by the prospective worker with data housed by the SSA and DHS.[91] But the new program calls for the protection of authenticated information through the use of

---

[82] MEISSNER & ROSENBLUM, *supra* note 3, at 10 ("Inaccurate verification allows bad-faith employers and unauthorized workers to go through the motions of compliance . . . while still violating the law. . . .").

[83] *Id*.

[84] *Electronic Employment Verification Systems*, *supra* note 33, at 1.

[85] The hearing was the third in a series of hearings addressing immigration reform, the problems with the "current paper-based system" and the proposals to improve EEV. *Id.*

[86] *Id*. at 36–37. The proposal would also create private-sector, government-certified companies to authenticate the identities of new employees through background checks and document screening tools. *Id*. at 37.

[87] *Id.* at 46 (statement of Jonathan Scharfen, Acting Director, USCIS).

[88] H.R. 2028, 111th Cong. § 103(b)(2)(A)(ii) (2009). The bill was introduced on April 22, 2009. On May 26, 2009, it was referred to the House Subcommittee on Immigration, Citizenship, Refugees, Border Security, and International Law where it currently remains. *H.R. 2028: New Employee Verification Act of 2009*, GOVTRACK.US, http://www.govtrack.us/congress/bill.xpd?bill=h111-2028 (last visited Nov. 19, 2010).

[89] H.R. 2028 § 101(1).

[90] *Id.* § 102(c)(1)(E).

[91] *Id.* § 103(b)(2)(A)(i).

biometric technology, a service to be provided by private third parties.[92] Employers who participate in SEEVS and follow required procedures, like those who participate in E-Verify, enjoy a presumption that the employer has not violated NEVA should DHS discover illegal workers.[93]

The bill also provides privacy protection for biometric data collected for SEEVS. First, it requires that stored biometric information be encrypted and segregated from other identifying information.[94] Second, it allows biometric data to be maintained and linked to identifying information of the new worker only if she consents.[95] Additionally, the bill requires that the worker's identifying and biometric information be removed from the system should she choose to cancel enrollment.[96]

III. SURVEYING BIOMETRICS

A. *Biometric Technologies*

Although the term may seem obscure, biometrics is nothing more than the measurement or analysis of unique physical or behavioral characteristics generally as a means to verify personal identity.[97] Prior to the 9/11 attacks, the use of biometric technologies had been increasing. Government agencies had already required the use of biometrics to control access to secure areas, and private companies had started using them to facilitate retail payment plans.[98] Of the many possible biometric technologies, eight were developed, tested, and placed in the public and private sectors.[99] But despite their presence, many people had little experience working with biometrics and the media had "virtually no knowledge" of biometric technology issues.[100]

The events of September 11, 2001 "led to an increase in calls for the use of biometrics."[101] Over the following years, biometrics evolved from a novel technology with limited application to a ubiquitous tool with a wide

---

[92] *Id.* § 103(b)(2)(A)(ii).
[93] *Id.* § 102(d)(3).
[94] *Id.* § 103(b)(2)(D)(i).
[95] *Id.* § 103(b)(2)(D)(ii).
[96] *Id.* § 103(b)(4)(C).
[97] *Biometrics Definition*, MERRIAM-WEBSTER ONLINE DICTIONARY, http://www.merriam-webster.com/dictionary/biometrics (last visited Nov. 19, 2010).
[98] WILLIAM SLOAN COATS ET AL., THE PRACTITIONER'S GUIDE TO BIOMETRICS 1 (William Sloan Coats ed., 2007).
[99] JOHN D. WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS: IDENTIFYING AND ADDRESSING SOCIOCULTURAL CONCERNS xv (2001) [hereinafter WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS]. Those eight include fingerprint, hand and finger geometry, facial recognition, voice recognition, iris scans, retinal scans, dynamic signature verification, and keystroke dynamics technology. *Id*.
[100] NAT'L SCI. & TECH. COUNCIL, BIOMETRICS IN GOVERNMENT POST-9/11: ADVANCING SCIENCE, ENHANCING OPERATIONS 7 (2008).
[101] COATS ET AL., *supra* note 98, at 1.

variety of applications across a broad range of industries.[102] In a post-9/11 world, biometrics has mainly served as a purported failsafe security device used by governments in border patrol management, law enforcement, and counterterrorism.[103] The federal government has focused biometric research, development, testing, and evaluation (RDT&E) efforts on four key areas: facial recognition, fingerprint identification, retinal identification, and multimodal biometric identification.[104] Multiple federal agencies "collaboratively planned, funded, and managed" these research activities, enabling the federal government to establish new, and to enhance existing, biometric technologies to improve U.S. security.[105]

1. *Facial Recognition*

Facial recognition is the automated process of recording the geometrically distinct features of the face, which are stored in a database, and then comparing them with samples for authentication.[106] An advantage of facial recognition is that "it can be easily confirmed by a system operator, such as a guard, by comparing a picture in [the] database" with an individual's facial features.[107] It is also "less intrusive" than any other biometric technology.[108]

Facial recognition systems represent about ten percent of the biometrics technology market share.[109] As the technology became more commercialized, the federal government began a series of evaluations for facial recognition systems.[110] Since 2000, there have been three evaluations, which have consecutively increased in size, difficulty, and complexity.[111] These evaluations provided a snapshot of facial recognition

---

[102] *Examine the Global Biometric Forecast to 2012*, MARKETWIRE (Oct. 20, 2008 1:51 PM), http://www.marketwire.com/press-release/Examine-the-Global-Biometric-Forecast-to-2012-911606.htm. One market research report estimates that the compound annual growth rate of biometric technologies will exceed twenty percent through 2012. *Id*.

[103] COATS ET AL., *supra* note 98, at 10–11.

[104] NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 13. Although NEVA does not require specific biometrics technologies, for the purpose of this Note I will only discuss the four technologies on which the federal government has increased RDT&E efforts. NEVA requires that the SEEVS "shall utilize the services of private sector entities," or enrollment providers, for "protection of the authenticated information [of a prospective worker] through [the use of] biometric technology." H.R. 2028, 111th Cong. § 103(b)(2)(A) (2009). Congress would likely evaluate potential biometric technology companies through a bidding process or by establishing a committee to evaluate existing biometric technologies and then requiring prospective vendors to provide a specific biometric technology or combination thereof.

[105] NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 12.

[106] WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS, *supra* note 99, at 16.

[107] COATS ET AL., *supra* note 98, at 4.

[108] *Id.*

[109] *Id*.

[110] NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 13.

[111] For more information on all three tests and their results, see FACE RECOGNITION VENDOR TEST, http://www.frvt.org/ (last visited Nov. 19, 2010) (describing the 2006 results of the Face Recognition Vendor Test results and providing links to the results of previous years).

capabilities and proved that some systems were comparable to, or better than, humans at facial recognition.[112] One of the most notable uses of facial recognition technology was at the 2001 Super Bowl in Tampa Bay. As attendees entered the stadium, the Tampa Bay Police Department used facial recognition technology to scan faces and compare them with face images in the police department's database.[113]

Of course, facial recognition technology is not without flaws. Environmental factors, such as lighting and the level of user cooperation, can adversely affect a system's performance.[114] Likewise, a user could fool a scanner by significantly altering her facial appearance.[115] Even under the best conditions, the performance of facial recognition systems is not high enough to a reasonable degree of reliability without severely constraining the system.[116] To address these and other concerns, the government sponsored two initiatives: the Facial Recognition Grand Challenge in 2004 and the Face Recognition Advanced Study Workshop in 2005.[117]

2. *Fingerprint Identification and Verification*

Fingerprint biometrics is one of the least intrusive and best known biometrics technologies.[118] It is an automated digital version of the older ink-and-paper method used by law enforcement agents.[119] A user scans her fingerprints to be read and checked against previously recorded copies.[120] Fingerprint technology represents almost half of the biometric technology market share.[121]

---

[112] P. JONATHON PHILLIPS ET AL., NAT'L INSTITUTE OF STANDARDS AND TECH., FRVT 2006 AND ICE 27 2006 LARGE-SCALE RESULTS 27 (2007) ("The ability of algorithms to recognize faces across illumination changes has made significant progress.").

[113] Jessica Reaves, *Tampa Gets Ready for Its Closeup*, TIME, July 16, 2001, *available at* http://www.time.com/time/nation/article/0,8599,167846,00.html.

[114] WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS, *supra* note 99, at 16; *see also* Ellen Nakashima, *FBI Prepares Vast Database of Biometrics; $1 Billion Project to Include Images of Irises and Faces*, WASH. POST, Dec. 22, 2007, at A1 (reporting that a German study found that current facial recognition technique had a sixty percent success rate during daylight but only a ten to twenty percent rate at night).

[115] John D. Woodward, *Biometric Scanning, Law & Policy: Identifying the Concerns—Drafting the Biometric Blueprint*, 59 U. PITT. L. REV. 97, 106 (1997) [hereinafter Woodward, *Biometric Scanning*].

[116] RUUD BOLLE ET AL., GUIDE TO BIOMETRICS 40 (2004).

[117] NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 14; *see also* P. JONATHON PHILLIPS ET AL., NAT'L INST. OF STANDARDS AND TECH., FRGC, OVERVIEW OF THE FACE RECOGNITION GRAND CHALLENGE 1 (2005) (describing the FRGC's goal to "achieve [an] increase in performance by pursuing development of algorithms" for the improvement of facial recognition technology). The FRASW was a two-day invitation-only workshop, where fifty-five participants were sequestered in intensive technical deliberations. FACE RECOGNITION ADVANCED STUDY RESEARCH, http://www.wvu.edu/~facerecognition/ (last visited Nov. 19, 2010).

[118] COATS ET AL., *supra* note 98, at 4.

[119] WOODWARD, JR. ET AL., ARMY BIOMETRICS APPLICATIONS, *supra* note 99, at 16.

[120] *Id.*

[121] COATS ET AL., *supra* note 98, at 4.

Capturing a fingerprint can be difficult because some people cannot generate clean fingerprint images and accuracy decreases with the user's age.[122] The quality of the fingerprint image captured is critical because the scanning devices use a complex set of algorithms to match captured fingerprints with stored fingerprint data.[123] All of the current four "livescan" fingerprint acquisition technologies available have some difficulty retrieving and storing digital fingerprints.[124]

Since the 9/11 attacks, the federal government has increased its efforts to advance and evaluate fingerprint recognition technology.[125] Through tests conducted in 2003 and 2004,[126] the government assessed the accuracy of algorithms used by fingerprint systems to measure and compare fingerprints and to evaluate which systems performed consistently.[127] The government has also worked to make capture devices faster and smaller.[128] Generally, a fingerprint biometrics program is employed for three reasons: law enforcement, fraud prevention, and access control.[129]

---

[122] *Id*.

[123] BOLLE ET AL., *supra* note 116, at 34 (describing the different matching approaches used by fingerprint authentication systems).

[124] *Id*. at 32–35. There are currently four common methods used to capture digital fingerprints and each presents its own challenge. First, optical methods capturing a reflected signal from the underside of a prism as the subject touches the top have trouble capturing images when fingertips are too wet or too dry. Second, CMOS capacitance converts different charge accumulations from the ridges and valleys of fingerprints into pixels. On the other hand, the capturing device is sensitive to scratching, electrostatic discharge, and mechanical failure. Third, thermal scanning measures temperature changes from the ridge-valley structure when a fingertip is swiped across a thermal scanner. Although less susceptible to wetness or dryness and static discharge, the copied images are not rich in value or range. Fourth, ultrasound sensing uses an ultrasonic beam scanned across the finger's surface, measuring the depth of the valleys from the reflected signal. Moisture and oils do not affect the sensitivity of these sensors, but they are very bulky and require longer scanning times than the other technology. *Id*. at 3.

[125] NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 13, 15.

[126] The government began the Fingerprint Vendor Technology Evaluation in 2003, testing segmentation fingerprint matching systems that measure a user's individual prints, requiring the system to separately capture a user's prints on each finger. Those tests revealed that top-performing systems performed consistently well over a variety of image types and data sources and confirmed the degree that additional fingers improve system accuracy. The system also revealed the degradation of accuracy caused by the collection of poor-quality prints. The government conducted a second series of evaluations in 2004, called the Slap Fingerprint Segmentation Evaluations. Slap Fingerprint analysis differs from segmentation fingerprints because the user must simultaneously press her four fingers of one hand onto a scanner or fingerprint card and the system captures the impressions of the four fingers. BRADFORD ULERY ET AL., SLAP FINGERPRINT SEGMENTATION EVALUATION 2004 ANALYSIS REPORT, EXECUTIVE SUMMARY 2 (2005); CHARLES WILSON ET AL., NAT'L INST. OF STANDARDS & TECH., FINGERPRINT VENDOR TECH. EVALUATION 2003: SUMMARY OF RESULTS AND ANALYSIS REPORT 2–3 (2004).

[127] WILSON ET AL., *supra* note 126, at 3.

[128] NAT'L SCI & TECH. COUNCIL, *supra* note 100, at 16 (describing the government's attempt to advance rolled-equivalent and slap devices in 2004 through the Fast Capture Rolled-Equivalent Finger/Palm Print Initiative).

[129] WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS, *supra* note 99, at 16.

3. *Iris Recognition*

The colored part of the eye surrounding the pupil, called the iris, is extremely rich in texture.[130] Iris recognition systems measure the pattern in the colored part of the eye, although the scan does not capture or measure the color.[131] The iris contains distributed immutable patterns, which form randomly.[132] No two irises are the same: the pattern in one's left eye is even different from the pattern in one's right eye.[133] Moreover, these patterns, like fingerprints, do not change over time.[134] Iris scanning devices account for almost ten percent of the biometric technology market share.[135]

While iris scanning can be highly accurate, it requires a high degree of cooperation—and patience—from the user.[136] Most commercial iris scanning systems "require the user to position his or her eyes within the field of view of a single narrow-angled camera."[137] Designing an iris capture device that is "convenient and unobtrusive" is a challenge.[138] The device needs to be sensitive enough to account not only for variations in ambient lighting from one situation to the next, but also for reflections of light from the eyeball, glasses, and contact lenses.[139] Thus, iris-scanning devices are one of the most expensive types of biometric technology.[140]

To improve the utility, performance, and ease-of-use of iris scanning, the federal government substantially increased its investments in the technology after the 9/11 attacks.[141] These investments have led to "iris-on-the-move" and "iris-at-a-distance" recognition systems.[142] In 2004,

---

[130] BOLLE ET AL., *supra* note 116, at 43.

[131] WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS, *supra* note 99, at 17.

[132] *Id.*

[133] *Id.* These patterns, like fingerprints, are the results of the developmental process, not genetics. BOLLE ET AL., *supra* note 116, at 43. The iris has proven to be a good biometric identifier with high discriminating properties. *Id.*

[134] Woodward, *Biometric Scanning*, *supra* note 115, at 103–04.

[135] COATS ET AL., *supra* note 98, at 4.

[136] Ravi Das, *Retinal Recognition: Biometric Technology in Practice*, 22 KEESING J. DOCUMENTS & IDENTITY 11, 14 (2007).

[137] BOLLE ET AL., *supra* note 116, at 44.

[138] *Id.*

[139] *See id.* (explaining that hard contacts create the biggest problem with reflected light pollution).

[140] COATS ET AL., *supra* note 98, at 4.

[141] NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 17; *see also* Ron Vetter, Editorial, *Authentication by Biometric Verification*, 43 COMPUTER, Feb. 2010, at 28, 28 (stating that "[i]n the past few years, government initiatives have spurred the growth of biometrics, and overall activities in biometric research have accelerated tremendously," and that "[t]his growth is due not only to increased interest in security concerns after 9/11, but also in response to privacy concerns regarding the confidential use of personal information being stored and transmitted across the Internet").

[142] Arun Ross, *Iris Recognition: The Path Forward*, 43 COMPUTER, Feb. 2010, at 30, 34. Other improvements have included increased standoff distances for accurate measurements, increased system performance (while also reducing size and cost), and the development of prototypes capable of acquiring and matching the iris of users while moving through a portal. NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 17–18.

John F. Kennedy International Airport in New York City installed an iris-scanning system for employees to access secure areas of the airport.[143]

4. *Multimodal Biometric Identification*

The previously-discussed biometric systems are unimodal systems, meaning they rely on evidence from a single source of information for authentication.[144] Multimodal biometric identification systems rely on multiple sources of information to establish identity.[145] The systems can fuse matching information between biometric data entered by the user and biometric data saved on databases.[146] Prior to the 9/11 attacks, the federal government had "begun efforts to develop automated, multimodal systems for identifying people at a distance."[147] Biometric technology combinations explored included "facial recognition, iris recognition, Doppler radar, infrared imagery, pulse and heartbeat recognition, and gait recognition."[148] By the end of 2003, some biometric systems were capable of recognizing users at up to 150 feet.[149]

5. *Other Feasible Biometric Options*

Although the federal government has invested significant research and development into four biometric technologies since the 9/11 attacks, recent developments may prompt Congress to consider other biometric technologies. Infrared vein scanning captures images of blood vessels in the back of the hand with infrared light and stores the picture on a template.[150] While the technology originally required scans of the entire hand or palm, Hitachi has developed a system that uses infrared LEDs and a CCD (charged couple device) camera to scan and capture vein patterns in the middle section of a finger, which it compares to a database associated with the application assigned to the finger.[151] One author notes that "92%

---

[143] Robin Feldman, *Considerations on the Emerging Implementation of Biometric Technology*, 25 HASTINGS COMM. & ENT. L.J. 653, 661 (2003); Ina Paiva Cordle, *Airports Focus on Limiting Workers' Access*, MIAMI HERALD, Mar. 14, 2004, at E1.

[144] These systems typically suffer from five problems because of their reliance on one type of data: (1) noise in sensed data—a scar on a finger or cold air affecting a voice or noise interference emanating from faulty scanning sensors; (2) intra-class variation—variations because the user is incorrectly interacting with a sensor or because the sensor is modified during the authentication; (3) inter-class similarities—the larger the pool of user information in a database, the more likely that multiple users will have features that overlap; (4) non-universality—the inability of biometric systems to pick up meaningful biometric data from poorly defined features; and (5): spoof attacks—fraudulent data or behavior by users. Arun Ross & Anil K. Jain, *Multimodal Biometrics: An Overview*, *in* PROCEEDINGS OF THE 12TH EUROPEAN SIGNAL PROCESSING CONFERENCE 1221, 1221 (2004).

[145] *Id.*

[146] *Id.* at 1221–22.

[147] NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 18.

[148] *Id.*

[149] *Id.*

[150] Woodward, *Biometric Scanning*, *supra* note 115, at 108.

[151] Kathy Kincade, *Vein Scanning Improves Door, Car, and Computer Security*, 44 LASER FOCUS WORLD, May 2008, at 17, 21.

of the financial institutions in Japan have adopted finger-vein biometric devices in their ATMs,"[152] demonstrating that the technology is a practical and affordable solution.

B. *Current Biometric Operational Activities by the U.S. Government*

Prior to the 9/11 attacks, the federal government used two major biometric systems: the FBI's Integrated Automated Fingerprint Identification System (IAFIS) and INS's Automated Biometric Integrated System.[153] Today, biometrics have permeated the operational activities of the Department of Defense (DOD), DHS, the Department of Justice (DOJ), and the State Department.

1. *Department of Defense*

After September 11, 2001, the DOD created a biometric collection and storage system compatible with IAFIS to lock down the identity of known or suspected terrorists.[154] Known as the Automated Biometrics Identification System (ABIS) and managed by the Biometrics Task Force (BTF),[155] the database consists of biometric information from individuals captured in Iraqi and Afghani war zones.[156] The resulting collaboration between the DOD and the FBI led to the discovery that many war criminals had prior criminal records in the United States.[157] Similar to SEEVS, the DOD used the biometric information to screen Iraqi personnel applying for selection into the Iraqi Police Academy. This system prevented known terrorists and insurgents from serving on the police force, ultimately leading to their recapture.[158] To date, the DOD uses facial recognition, fingerprints, iris recognition, and palm imaging data.[159]

---

[152] *Id.* at 24.

[153] NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 23.

[154] Ellen Nakashima, *Post-9/11 Dragnet Turns Up Surprises; Biometrics Link Foreign Detainees to Arrests in U.S.*, WASH. POST, July 6, 2008, at A01.

[155] BTF was created in 2006 as a result of a DOD reorganization that consolidated the Biometrics Management Office (BMO), which managed and regulated the Department's biometric technologies, and the Biometrics Fusion Center (BFC), which was responsible for evaluating and procuring biometrics technologies that were compatible with the Department's information systems. *See DoD Biometrics Reorganization Takes Shape*, 2 BIOMETRIC BULL., Mar.–Apr. 2006, http://www.biometrics.dod.mil/Newsletter/issues/2006/March/v2issue2_a1.htm (discussing the consolidation of the BMO and the BFC into the BTF); *see also* BIOMETRICS TASK FORCE, ANNUAL REPORT FY07 6 (2007), *available at* www.biometrics.dod.mil/Files/Documents/AnnualReports/fy07.pdf (discussing the creation of ABIS and ABIS's purpose).

[156] *See* Nakashima, *supra* note 154 (detailing the use of ABIS for maintaining records on Iraqi and Afgahni detainees).

[157] *Id.*

[158] *See* BIOMETRICS TASK FORCE, *supra* note 155, at 7 (noting that the system revealed that some applicants to the Iraqi Police Academy had records as terrorists or insurgents).

[159] *Biometrics History Timeline*, BIOMETRICS IDENTITY MGMT. AGENCY, http://www.biometrics.dod.mil/References/Biometrics_Timeline.aspx (last visited Nov. 19, 2010).

2. *Department of Homeland Security*

DHS, created after the 9/11 attacks, has statutory and regulatory mandates to incorporate biometrics.[160] Because DHS's main function is to keep terrorists out of the United States, as well as to welcome international travelers into U.S. ports on a daily basis, DHS "incorporate[s] biometrics into identity documents for the purpose of freezing identity, searching waitlists, conducting criminal background checks, reducing fraud, improving border and transportation security, and granting benefits and credentialing."[161] DHS also provides biometric identification and analysis services to immigration and border management agencies, law enforcement departments, and intelligence communities to aid in the assessment of an individual's risk to the United States.[162] The vast majority of the data collected is in the form of digital fingerprints and photographs.[163] DHS also manages the Transportation Worker Identification Credentials (TWIC) program, which uses biometrics to screen and verify the identities of transportation workers, who are allowed access to the most sensitive parts of the nation's transportation infrastructure.[164] Congress established the TWIC through the Marine Transportation Security Act, which requires the Transportation Security Administration to collect a transportation worker's ten fingerprints, biographical information, photograph, employer information, and other appropriate information in exchange for access to secure areas of port facilities.[165]

3. *Department of Justice*

Prior to September 11, 2001, the DOJ, through the FBI, maintained IAFIS, which, at the time of its creation was "the largest and most advanced biometric database in the world"; IAFIS held fingerprint data information linked to criminal histories from all fifty states and the U.S.

---

[160] *See, e.g.*, Enhanced Border Security and Visa Entry Reform Act of 2002, Pub. L. No. 107-173, § 303, 116 Stat. 543, 554 (codified at 8 U.S.C. § 1732 (2006)) (requiring that each country participating in a visa waiver program "shall certify . . . that it has a program to issue to its nationals machine-readable passports that are tamper-resistant and incorporate biometric and document authentication identifiers"). DHS was created by merging twenty-two different government organizations into a single department. Because many of these organizations maintain autonomy and responsibility for planning and managing their own biometric systems, DHS created the Biometrics Coordination Group (BCG) to ensure department-wide coordination. *History: Who Became Part of the Department?*, U.S. DEP'T OF HOMELAND SEC. (Apr. 11, 2008), http://www.dhs.gov/xabout/history/editorial_0133.shtm.

[161] NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 28.

[162] *Id.* at 29.

[163] U.S. DEP'T OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT FOR THE BIOMETRIC STORAGE SYSTEM 3 (2007).

[164] TRANS. SEC. ADMIN., U.S. DEP'T OF HOMELAND SECURITY, PRIVACY IMPACT ASSESSMENT: TRANSPORTATION WORKER IDENTIFICATION CREDENTIAL (TWIC) PROTOTYPE 2 (2004).

[165] *Id.*

territories.[166] After the 9/11 attacks, Congress, making national security as important as criminal investigation, authorized the U.S. Attorney General to expand IAFIS and other biometric services into the civil sector.[167] In 2007, the FBI announced that it planned to spend over one billion dollars to compile a biometric database, labeled Next Generation Identification (NGI), that would consist of digital face images, fingerprints, palm patterns, iris scans, and voice data.[168] As of March 2010, NGI was going through contractor testing and is scheduled to begin operation in early 2011.[169] The FBI also coordinates with DHS to make both Departments' databases interoperable.[170] The FBI collaborates with the DOD obtaining data received from military operations abroad and providing data collected by the FBI.[171]

4. *State Department*

The State Department has also expanded biometric efforts since the 9/11 attacks. The Biometric Visa Program (BioVisa) mandates biometric screening for visa applicants and requires the Department to use biometric identifiers for all visas issued to aliens.[172] In 2008, the State Department transitioned BioVisa from the collection of two fingerprints to ten.[173] These prints are then scanned against IAFIS, which also uses a ten-fingerprint system.[174] BioVisa also uses facial-recognition technology for persons exempt from fingerprints during the application process.[175]

---

[166] NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 37.

[167] *Id.*

[168] Calvin Biesecker, *Lockheed Martin Nabs FBI Contract To Develop Multi-Modal Biometric Database*, 237 DEF. DAILY, Feb. 13, 2008.

[169] *NGI Program Holding Close to Schedule, FBI Says*, 6 TERROR RESPONSE TECH. REP., Mar. 3, 2010.

[170] NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 39.

[171] *Id.* The FBI and the Department of Defense, for example, established the Automated Fingerprint Identification System for the Afghani government, with fingerprint data collected on a ninety-day mission in Afghanistan. *Id.*

[172] Amendment to the Biometric Visa Program, 75 Fed. Reg. 39,323, 39,323 (July 8, 2010).

[173] *Interrupting Terrorist Travel: Strengthening the Security of International Travel Documents: Hearing Before the Subcomm. on Terrorism, Tech. and Homeland Sec. of the S. Comm. on the Judiciary*, 110th Cong. 3 (2007) (statement of Paul Morris, Executive Director, U.S. Customs and Border Protection).

[174] *See id.* ("[T]he biometric and biographic data are checked against watch lists of known or suspected terrorists, outstanding wants and warrants, immigration violations, and other criminal history information."); *see also* NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 46 (describing the search process involving fingerprint scans and IAFIS's criminal master file).

[175] Individuals exempt from fingerprint collection include diplomats, certain government officials, children under age fourteen, and persons over age eighty. NAT'L SCI. & TECH. COUNCIL, *supra* note 100, at 45. Their photographs are then checked against photograph watch lists to combat visa fraud and catch wanted criminals or terrorists. *Id.*

IV. LEGAL IMPLICATIONS OF NEVA AND THE COLLECTION OF BIOMETRIC DATA

If enacted, NEVA would require the government to incorporate biometrics data into SEEVS and E-Verify and to collect biometric data from prospective workers. This collection raises the same legal issues that arise when the government collects any information from its citizens: whether such collection constitutes a violation of a prospective worker's Fourth Amendment right to be free from unwarranted and unreasonable searches and seizures.[176] The Fourth Amendment gives "the people [the right] to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[177] Just as the Fourth Amendment ordinarily requires that a police officer have a search warrant to search a dwelling, the Supreme Court has stated that "'no less could be required where intrusions into the human body are concerned. . . .'"[178] The Court has also noted that "a Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable."[179] Because biometric technology involves collecting data from parts of an individual's body and may reveal private medical information about the individual,[180] the use of such technology could implicate the Fourth Amendment in two ways: (1) gathering biometric evidence may constitute an intrusion into—and therefore a Fourth Amendment search of—a person's body; or (2) gathering biometric evidence may reveal private medical information, violating an established societal expectation of privacy.

A. *Gathering Biometric Data Through E-Verify Does Not Appear To Be a Fourth Amendment Search*

The Supreme Court has held that fingerprinting is subject to the requirements of the Search and Seizure Clause of the Fourth Amendment.[181] In *Davis v. Mississippi*, the Meridian, Mississippi police,

---

[176] The United States Supreme Court has yet to address whether the collection of biometric data constitutes a search or seizure under the Fourth Amendment. The Court has ruled that detaining a suspect in a criminal investigation for the sole purpose of collecting fingerprints is a seizure under the Fourth Amendment. Davis v. Mississippi, 394 U.S. 721, 726 (1969). Collection of biometric data through E-Verify, however, would not fall under the *Davis* ruling because the data would not be used for criminal investigatory purposes and the collection would not occur during a detainment.

[177] U.S. CONST. amend. IV; *see also* Kyllo v. United States, 533 U.S. 27, 31 (2001) (quoting the above text of the Fourth Amendment and noting that "'[a]t the very core' of the Fourth Amendment 'stands the right of a man to retreat into his home and there be free from unreasonable governmental intrusion'" (quoting Silverman v. United States, 365 U.S. 505, 511 (1961))).

[178] Winston v. Lee, 470 U.S. 753, 761 (1985) (quoting Schmerber v. California, 384 U.S. 757, 770 (1966)).

[179] *Kyllo*, 533 U.S. at 33 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

[180] *See infra* notes 232–37 and accompanying text.

[181] United States v. Dionisio, 410 U.S. 1, 4 (1973) (citing *Davis*, 394 U.S. at 724).

without warrants, detained at least twenty-four African American teenagers at police headquarters when a rape victim could only describe her assailant as a black youth.[182] The police found fingerprints on the sill and borders of a window that the victim alleged the assailant had used to enter her home.[183] The police detained the teenagers, questioned them, fingerprinted them, and released them without charge.[184] Davis, who had previously worked as a "yard boy" for the victim, was eventually detained because a set of his fingerprints—and a second set taken after he was again detained overnight in jail in Jackson, Mississippi—matched the prints on the window.[185] The police used the prints at Davis's trial over his objection, and he was subsequently convicted of rape.[186]

Because the fingerprints were captured during an illegal detention, the Court overturned Davis's conviction, reasoning that "[d]etentions for the sole purpose of obtaining fingerprints are no less subject [than arrests] to the constraints of the Fourth Amendment."[187] The Court did note, however, that some narrowly-defined detentions without probable cause *might* comply with the Fourth Amendment.[188] But the Court declined to determine whether "narrowly circumscribed [criminal investigation] procedures" for obtaining fingerprints without probable cause would meet Fourth Amendment requirements.[189]

Although *Davis* put detentions for the sole purpose of collecting fingerprints for criminal investigation under the Fourth Amendment's constitutional umbrella of protection against unreasonable searches, in the context of seeking employment, where the prospective worker is not detained and her fingerprints are not used for criminal investigation, the

---

[182] *Davis*, 394 U.S. at 722.

[183] *Id.*

[184] *Id.*

[185] *Id.* at 723.

[186] *Id.*

[187] *Id.* at 727. The Court relied on this same precedent in *Hayes v. Florida*. 470 U.S. 811, 814 (1985). In that case, police went to the house of the alleged assailant and threatened to arrest him if he did not cooperate and go to the police station with them to be fingerprinted. *Id.* at 812. When the prints matched those at the crime scene, Hayes was subsequently arrested, charged, and convicted. *Id.* at 813. The Court held that there was no probable cause to arrest Hayes, that his fingerprints were taken without consent, and that, therefore, the fingerprints "were the inadmissible fruits of an illegal detention" in violation of the Fourth Amendment. *Id.*

[188] *Davis*, 394 U.S. at 727.

[189] *Id.* at 728. The Court noted that "[d]etention for fingerprinting may constitute a much less serious intrusion upon personal security than other types of police searches and detentions" because capturing fingerprints "involves none of the probing into an individual's private life and thoughts that marks an interrogation or search." *Id.* at 727. Because the police only need one set of prints, the detention could not be employed repeatedly to harass an individual, and because there is little danger of fingerprints being destroyed, the police could schedule the detention at a convenient time for the individual. *Id.* This dicta suggests that gathering fingerprints for the purpose of criminal investigation *may not* constitute a Fourth Amendment seizure in some instances, narrowing the *Davis* holding to, at the very least, the facts of that case. Further, now that fingerprints can reveal medical information about an individual, taking images of them may implicate more than just identification.

Fourth Amendment likely would not apply. In *Davis*, the state forced the defendant to record his fingerprints for its criminal investigation against him. NEVA, however, does not force a prospective worker to give her fingerprints. Rather, she would exchange them for the opportunity of employment. Under this rationale, it is likely that a court would find that requiring an applicant to submit biometrics data for employment does not constitute a search under the Fourth Amendment.

The Third Circuit Court of Appeals has already made a similar finding. In *Trade Waste Management Ass'n v. Hughey*,[190] the Third Circuit upheld a New Jersey law that required prospective licensees to disclose information, including fingerprints, in order to obtain a license to dispose of solid and hazardous waste within the state.[191] The law had been created to prevent organized crime from having ownership interests in the waste-disposal industry.[192] The fingerprints were taken from prospective licensees and then crosschecked with the state and the FBI criminal databases.[193] The statute required that the state collect fingerprints from business owners, stockholders, or beneficiaries of company funds to them.[194] The discovery of convictions of, or pending charges for, certain crimes would result in a denial of the company's application.[195]

The plaintiffs alleged that the fingerprinting requirement violated their constitutional right to privacy.[196] The Third Circuit, however, found that the statute's "fingerprinting requirement . . . . [wa]s not involuntary in the [F]ourth [A]mendment sense. It [wa]s required only as a condition for obtaining or keeping a license to engage in a business that the state may license."[197] Moreover, the State may compel disclosure of private information if its interest in such disclosure outweighs the individual's privacy interests, and because the law was rationally related to the investigation of the licensees' qualifications, which the court found to be a compelling governmental interest, the court upheld the law.[198]

Just as the statutory scheme for the licensee program established in *Trade Waste* used fingerprints to prevent participants in organized crime from having ownership interests in the waste disposal industry, so too would NEVA utilize the same technology to create an applicant-filter program aimed at decreasing the "economic magnet" that draws illegal

---

[190] 780 F.2d 221 (3d Cir. 1985).
[191] *Id.* at 228, 239.
[192] *Id.* at 223.
[193] *Id.* at 228, 233.
[194] *Id.* at 224–25, 233.
[195] *Id.* at 225–26. These crimes included murder, kidnapping, gambling, robbery, bribery, extortion, criminal usury, arson, burglary, theft, and other related crimes. *Id.*
[196] *Id.* at 233.
[197] *Id.* at 234.
[198] *Id.*

immigrants into the United States.[199] The legal principles of *Trade Waste* should also apply to SEEVS. The requirement that prospective employees submit to fingerprint scans would not constitute a Fourth Amendment search because the fingerprints would be a condition precedent to obtaining employment. Such a prerequisite to employment is not unlike requiring suspicionless drug-testing of employees who apply for promotions, which the Court has held is a reasonable Fourth Amendment search.[200] Also, unlike in *Davis* or in *Hayes*, the government would not detain or fingerprint an applicant without consent.

Likewise, SEEVS is rationally related to the government's interest in securing national borders and discouraging illegal immigration.[201] Fingerprinting would simplify the process of determining whether an applicant is the person she claims, and would make it tougher for illegal immigrants to commit fraud, because it would be harder to copy and use a person's fingerprint than it presently is to copy and use a person's social security number. The program would also relieve employers of the burden of determining whether a person resembles the picture presented on her legal documents, and it has the potential to alleviate errors that would only occur in a system based purely on name and numbers.[202]

Like fingerprint collection, capturing iris images would also likely not constitute a Fourth Amendment search or seizure.[203] The scan itself commits no more of an intrusion into the body than a fingerprint scan. Although the iris is a sub-dermal organ, the technology only measures and records what is visible through the cornea.[204] The process of recognition appears less intrusive than a fingerprint scan to the user because, unlike fingerprint or palm recognition, the user does not have to place the part scanned on anything—she only needs to direct her eyes in a specified direction.[205] Iris scans are also much less intrusive than retinal scans,

---

[199] *See* Harper, *supra* note 5, at 4 (explaining that the "logic" Congress used in enacting the Immigration Reform and Control Act was to "reduce the strength of [the] country's economic 'magnet'" by "making it illegal to hire an illegal immigrant").

[200] Nat'l Treasury Emps. Union v. Von Raab, 489 U.S. 656, 679 (1989).

[201] *See supra* note 7 and accompanying text.

[202] *But see* Feldman, *supra* note 143, at 663 (arguing that "[n]o biometric technique is completely accurate"). Fingerprint scans could introduce new, complex error problems, and while generally reliable, they may be misread if the user puts her finger at a different angle or pressure than the fingerprint on file. *Id.* An automated finger scanner would be only as good as the humans who ran the system, and human error will undoubtedly still play a role in SEEVS. *Id.* at 664.

[203] There are no federal cases that address the question of whether an iris scan would constitute a search under the Fourth Amendment.

[204] *See* WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS, *supra* note 99, at 17 ("Iris scanning measures the iris pattern in the colored part of the eye.").

[205] Of course, no matter how intrusive the process of iris recognition *actually* is, undoubtedly the practice may *feel* more intrusive because the process carries a negative connotation, generated by Hollywood movies such as *Minority Report* and *Demolition Man*. *See* Feldman, *supra* note 143, at 660–61 n.43 (listing movies and television shows that have portrayed iris scans). The American public may therefore erroneously believe that iris scanning impedes on the private sphere more than

which require measurements and copies of the veins contained inside the eye wall.[206] As the technology advances, recognition should take less time and be accurate at longer distances.

Unlike fingerprints or patterns around the eye, an individual's facial features are exposed "regardless of the cooperation or compulsion of the owner."[207] Consequently, the Supreme Court has held that "facial scars, birthmarks, and other facial features" are "in plain view" and therefore are not protected by the Fourth Amendment.[208] Moreover, according to the Second Circuit, there is no reasonable expectation of privacy as to the features on one's face.[209] It follows, then, that regardless of whether a person is wrongfully detained or not, an individual's facial features will almost never be protected under the Fourth Amendment. If SEEVS utilizes a facial recognition system, such a system should not fall within the purview of a Fourth Amendment search.

B. *If Gathering Biometric Data Through E-Verify Is a "Search," It Is a Minimal Intrusion to Prospective Workers and Involves a Governmental Interest Outweighing Any Privacy Interest*

Even if a court were to find that requiring an applicant to submit biometric data for employment constitutes a search under the Fourth Amendment, it may also find that a biometric submission would fall under one of two exceptions: (1) administrative searches; or (2) "special needs" searches.

1. *The Administrative Search*

Administrative searches include inspections of closely-regulated businesses and extend to other routine regulatory investigations.[210] For example, in *New York v. Burger*,[211] the Court held that a business owner's expectation of privacy is attenuated with respect to his commercial property, where the business is "closely regulated."[212] In that case, a

---

fingerprint collection, even though current reports suggest that that data is used no differently than fingerprint recognition. *See* WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS *supra* note 99, at 26–27 (discussing a study, which suggests that managers of voluntary biometrics programs had no concern for stigma, but that managers in mandatory biometrics programs may have had some concern for stigma).

[206] *See* WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS, *supra* note 99, at 17 (explaining the differences between iris scans and retinal scans).

[207] United States v. Mara, 410 U.S. 19, 27 (1973).

[208] *See id.* at 26 (citing United States v. Doe, 457 F.2d 895, 898 (2d Cir. 1972)) (noting that, in *Davis*, the Court held that fingerprints were protected by the Fourth Amendment, but that other courts have found that facial features do not receive the same protection).

[209] *Doe*, 457 F.2d at 898.

[210] *See* United States v. Kincade, 379 F.3d 813, 823 (9th Cir. 2004) (noting that "'administrative' searches . . . include[] inspections of closely-regulated businesses").

[211] 482 U.S. 691 (1987).

[212] *Id.* at 700.

warrantless search of a vehicle junkyard was upheld as reasonable because of the diminished privacy interest of the business owner in his commercial property and the state's substantial interest in curbing automobile thefts.[213]

If a court upheld E-Verify as an administrative search, that court would most likely find that the substantial governmental interest outweighed an individual's privacy interest. First, when a worker submits her personal information to an employer, she arguably has a lower expectation of privacy. She surrenders her home address, social security number, driver's license number, birth certificate information, and other identifying documents to her employer, the SSA, and the IRS. Even if her information may never leave these agencies, the worker still subjects herself to a lower expectation of privacy. Likewise, the government's interest in preventing illegal employment increases substantially in the employer-employee context.[214] Given the degree of intrusion from a scan of the finger, face, or iris, and the requirement of House Resolution 2028 that all biometric information collection comport with privacy legislation,[215] such an analysis may very well fall against the worker.

It is unlikely, however, that a court will find that the employer-employee relationship and hiring process is a "closely regulated" business. House Resolution 2028 would expand to employers already participating in E-Verify, which include those not "closely regulated."[216] For an administrative search exception to apply, the business must be "closely regulated," meaning "[c]ertain industries have such a history of government oversight that no reasonable expectation of privacy . . . exist[s] . . . ."[217] To apply to the hiring process, a court would need to stretch the definition of "closely regulated" business beyond its historical context to incorporate a general business process. One would also have to argue that the hiring process has a history of government oversight, which has created little or no expectation of privacy. It is unlikely that such an argument would be successful.

2. *"Special Needs" Searches*

Justice Blackmun established the "special needs" exception in *New Jersey v. T.L.O.*,[218] which upheld the constitutionality of a school administrator's search of a student's purse after she had been observed smoking in a school restroom.[219] After *T.L.O.*, courts use the special needs

---

[213] *Id.* at 713–14.
[214] *See supra* notes 7 and accompanying text.
[215] *See supra* notes 94–96 and accompanying text.
[216] H.R. 2028, 111th Cong. § 102(a)(2) (2009).
[217] New York v. Burger, 482 U.S. 691, 700 (1987) (internal quotation marks omitted).
[218] 469 U.S. 325, 351 (1985) (Blackmun, J., concurring).
[219] *See id.* at 347 (majority opinion) (stating that the administrator's decision to open the student's bag and "the search resulting in the discovery of the evidence of marihuana dealing" were reasonable).

doctrine to justify, in narrow contexts, searches made without a warrant or individualized suspicion based upon "a careful balancing of governmental and private interests."[220] The Court limits this test to "those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable."[221] For the special needs doctrine to apply, the primary purpose of a search conducted by a school official must constitute a special need beyond the normal need for law enforcement, and must outweigh the privacy interest at stake and the character of the intrusion.[222]

A court may find that extracting biometric data to determine a prospective worker's citizenship status would be a "special needs" search and therefore constitutionally permissible. First, Congress has a strong interest in policing the national border.[223] SEEVS's purpose advances this interest because it should substantially decrease an individual's chances of circumventing identification procedures and acquiring employment in the United States.[224] Second, the character of the intrusion is minimal. Biometric automated systems may capture digital images of fingerprints and irises, but those images are stored in the form of an algorithm and are only used to compare with fresh data samples obtained by a user. E-Verify would obtain biometric information for administrative purposes—determining whether a prospective worker is hirable—and would not be used as a tool of law enforcement. The biometric information would be compared to information in a database, and, when there is no match, the only consequence is a final nonconfirmation—the employer cannot legally hire the worker.[225]

3. *"Totality of the Circumstances" Analysis*

The Supreme Court has recently expanded its Fourth Amendment jurisprudence by using a "totality of the circumstances" test to assess the constitutionality of searches conducted without a warrant or individualized

---

[220] *Id.* at 351 (Blackmun, J., concurring); *see also* Ric Simmons, *Searching for Terrorists: Why Public Safety Is Not a Special Need*, 59 DUKE L.J. 843, 863–64 (2010) (explaining that "[i]n his concurrence, Justice Blackmun set out a test that would be used in future cases").

[221] *T.L.O.*, 469 U.S. at 351 (Blackmun, J., concurring).

[222] *See* Simmons, *supra* note 220, at 864–865 (explaining that the Court later loosened the special needs doctrine to consider other factors such as expectation of privacy and the intrusiveness of the invasion).

[223] *See* United States v. Martinez-Fuerte, 428 U.S. 543, 566–67 (1976) (finding that the government's interest in conducting suspicionless fixed-checkpoint vehicle stops outweighed a private individual's Fourth Amendment interests).

[224] *See supra* notes 129 and 143 and accompanying text.

[225] Note, however, that if the employer hires the worker, the worker may be detained if she is on the employer's premises during a DHS raid. *See* MEISSNER & ROSENBLUM, *supra* note 3, at 4 (explaining how E-Verify works); Harper, *supra* note 5, at 5 (same).

suspicion.[226] In *United States v. Knights*[227] and *Samson v. California*,[228] the Court declined to undertake a special needs analysis and instead examined the "totality of the circumstances" of the search of a probationer's apartment with only reasonable suspicion and the search of a parolee without any suspicion.[229] Both searches under this lesser standard were found to be reasonable.[230] Although the subject matter of these cases falls outside the scope of this Note, this expanded analysis is worth highlighting because it "has provided a new method to judge the Fourth Amendment constitutionality of government searches."[231] If a court employs a totality-of-the-circumstances analysis in determining whether NEVA's biometric requirement constitutes a search, it is likely that the relatively non-invasive and brief nature of capturing biometric information would surmount the reasonableness threshold. A court, however, has yet to use this analysis outside of the parolee-probationer search context.

C. *Creating a Biometric Database Would Not Violate Privacy Expectations*

Unlike social security numbers, pin numbers, or passwords, biometrics may contain medical information about an individual.[232] The iris or retina, for example, could reveal health conditions such as diabetes, arteriosclerosis, and hypertension.[233] Certain studies have suggested a link between fingerprint patterns and homosexuality and that a number of chromosomal disorders can affect the patterns of ridges in the finger.[234]

---

[226] Charles J. Nerko, Note, *Assessing Fourth Amendment Challenges to DNA Extraction Statutes After* Samson v. California, 77 FORDHAM L. REV. 917, 926 (2008).

[227] *See* United States v. Knights, 534 U.S. 112, 121–22 (2001) (holding that a warrantless search of a probationer's apartment, supported by reasonable suspicion and authorized by a condition of probation, was reasonable under the Fourth Amendment given the totality of the circumstances, and stating that "[a]lthough the Fourth Amendment ordinarily requires the degree of probability embodied in the term 'probable cause,' a lesser degree satisfies the Constitution when the balance of governmental and private interests makes such a standard reasonable").

[228] *See* Samson v. California, 547 U.S. 843, 852, 857 (2006) (holding that a suspicionless search of a parolee did not violate the Fourth Amendment and that the "totality of the circumstances" must be examined to determine whether a search is reasonable under the Fourth Amendment).

[229] Nerko, *supra* note 226, at 926–27.

[230] *Id.* at 926–28.

[231] *Id.* at 930.

[232] *See* WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS, *supra* note 98, at 30 (stating that "[b]ecause biometrics are inherent to the individual, researchers are likely to try to link medical predispositions, behavioral types, or other characteristics to particular biometric patterns"); *see also* Woodward, *Biometric Scanning*, *supra* note 115, at 115–17 (arguing that biometric scanning may prompt various legal and policy concerns because it may incidentally capture information about individuals' medical history).

[233] Woodward, *Biometric Scanning*, *supra* note 115, at 115.

[234] *See, e.g.*, P.E. Natekar & F.M. DeSouza, *Digital Dermatoglyphics in Leprosy*, 9 ANTHROPOLOGIST 63, 65 (2007) (discussing the results of a study that revealed leprosy may affect the development of fingerprint ridges); Christopher Hernandez, *Sexuality Is Genetic, Professor Argues*, DAILY PRINCETONIAN, Oct. 12, 2006, *available at* http://www.dailyprincetonian.com /2006/10/12/16168/ (stating that "researchers . . . have examined fingerprint patterns, hypothalamus

Should such information be disclosed when a user submits biometric information, it would likely implicate a societal expectation of privacy and constitute a "search" under the *Katz* doctrine.

Current technology is not capable of disclosing private medical information from the biometric data collected.[235] Existing biometric systems do not observe biometric data as a human would, but rather "translate information into a mathematical construction that has no physiological meaning."[236] For such capabilities to exist, it would most likely require a huge shift in the concept of biometric scanning technology.[237] Only then will those concerns be addressed.

Even if SEEVS could reveal private medical information about a user, NEVA requires that all biometric data collected be encrypted and segregated from the worker's identifying information unless the worker requests otherwise.[238] SEEVS must also conform to existing privacy laws.[239] NEVA gives the worker the right to cancel enrollment at anytime after the authentication process is over.[240] When requested, the cancellation removes the worker's biometric information from SEEVS without prejudice.[241]

Some courts allow storage of other kinds of information. For example, several circuit courts have upheld the collection and storage of DNA samples from convicts as reasonable under the Fourth Amendment.[242] In

---

size, the size differential between the second and fourth digit of the hand, pheromones and even the sexuality of sheep").

[235] *See* Feldman, *supra* note 143, at 667 (explaining that "[i]t would take a significant technological shift . . . to go from current biometric systems to systems that reveal disease or other health information").

[236] *Id.* Retinal scans, for example, do not take images of the retina. Instead, they scan the retina in a circle to create a one-dimensional pattern, which is then compared to other patterns contained in a database. *Id*. Likewise, fingerprint scans are not based on direct comparisons of the images of fingerprints. The system measures the arches and patterns of the fingers and formulates an algorithm, which it then uses to determine if a fingerprint matches any print stored in the database. *See* WOODWARD, JR. ET AL., ARMY BIOMETRIC APPLICATIONS, *supra* note 99, at 16 (explaining that no print of the finger is taken and that fingerprint sensors measure the spatial geometry of the finger).

[237] Feldman, *supra* note 143, at 667.

[238] H.R. 2028, 111th Cong. § 103(b)(2)(D) (2009).

[239] *Id.* § 103(c)(3).

[240] *Id.* § 103(b)(4)(C).

[241] *Id.*

[242] *See* United States v. Sczubelek, 402 F.3d 175, 177 (3d Cir. 2005) (holding that "under Fourth Amendment reasonableness standard for analyzing the constitutionality of government searches and seizures, the collection of DNA samples from individuals on supervised release is constitutional"); United States v. Kincade, 379 F.3d 813, 839 (9th Cir. 2004) (concluding that "compulsory DNA profiling of qualified federal offenders is reasonable under the totality of the circumstances"); United States v. Kimler, 335 F.3d 1132, 1146 (10th Cir. 2003) (finding that "[t]he DNA Act, while implicating the Fourth Amendment, is a reasonable search and seizure under the special needs exception to the Fourth Amendment's warrant requirement because the desire to build a DNA database goes beyond the ordinary law enforcement need"); Roe v. Marcotte, 193 F.3d 72, 75, 79 (2d Cir. 1999) (finding that a "reasoned interpretation of the 'special needs' doctrine support[ed] the constitutionality" of a Connecticut statute that required, prior to the release of persons convicted of certain crimes, the

those cases, the courts found that the government's substantial interest in collecting DNA samples from convicts, parolees, and probationers outweighed the very limited expectation of privacy that a convict, parolee, or probationer might have.[243] Although the government's interest in collecting biometric information from prospective workers is arguably less than its interest in collecting DNA samples from convicts, so too is NEVA's method of collection. In those cases, the government was collecting blood and tissue samples, while E-Verify would simply scan the image of a worker's fingerprint or iris. Because NEVA's method of collection is substantially less intrusive than that required by the DNA Act, a court, using the totality-of-the-circumstances test, could conclude it is a reasonable search under the Fourth Amendment.

V. CONCLUSION

Biometrics presents a practical solution to the large gaps that plague a crucial step in the worker verification process, namely, whether a worker is who she claims to be. Given enough resources, E-Verify has the potential to dramatically decrease the "employment magnet" that purportedly draws illegal immigrants into the United States. First, defrauders will find it more difficult to imitate biometric information. While biometrics will undoubtedly not end employment fraud, it will substantially discourage the majority of defrauders, who are capable of undermining existing verification procedures, and increase the security of personal identification. Second, biometrics will also relieve the employer's burden of on-the-spot worker identity verification. Instead of comparing document images of the worker with the person presenting them, an employer need only use SEEVS's biometric option to legally comply with NEVA. Third, because a biometric scan likely would not constitute a search under the Constitution, mandating SEEVS would not implicate Fourth Amendment protections. Existing technological capabilities and NEVA's privacy compliance requirement would ensure a worker's constitutional privacy; personal identity would not be compromised, while still maintaining a high level of accuracy.

Before Congress can employ such a system, however, several concerns must be addressed. Biometrics is still prone to human mistake and abuse. The current E-Verify infrastructure, which was created for a small voluntary program, would strain under a national mandate that would draw in millions of new employers and workers. Americans are also likely to disapprove of a biometrics requirement because of the stigma associated

---

collection of blood for "DNA . . . analysis to determine identification characteristics specific to the person").

[243] *Sczubelek*, 402 F.3d at 177; *Kincade*, 379 F.3d at 839; *Kimler*, 335 F.3d at 1146; *Marcotte*, 193 F.3d at 79–80.

with the government's use of the technology and ignorance of its limitations. If it hopes to successfully implement any biometrics recording regime, Congress first needs to educate the public on the technology's capabilities, and the system's weaknesses and rates of error would have to be mitigated. No doubt, a biometric employment verification system will require cooperation and patience from employers and workers, but it has the potential to significantly curb an illegal worker's ability to gain employment within the United States.